

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2017

Date filed: February 23, 2018

Name of company covered by this certification: T-Systems North America, Inc.

Form 499 Filer ID: 820820

Name of signatory: Bertus Cilliers

Title of signatory: Vice President: Finance

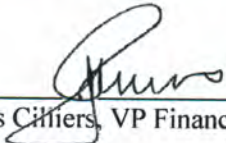
I, Bertus Cilliers, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject to enforcement action.

Signed 
Bertus Cilliers, VP Finance, T-Systems North America, Inc.

Date February 15, 2018

T-SYSTEMS NORTH AMERICA INC.

STATEMENT REGARDING CUSTOMER PROPRIETARY NETWORK INFORMATION OPERATING PROCEDURES

February 14, 2018

This statement is filed on behalf of T-Systems North America, Inc. ("TSNA" or "Company") pursuant to 47 C.F.R. § 64.2009(e) to demonstrate how TSNA's operating procedures are designed to ensure compliance with the Commission's CPNI rules.

Certification

TSNA requires a corporate officer to act as agent for the company and sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with applicable CPNI rules. TSNA's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

TSNA CPNI Protection Policy

TSNA has implemented a CPNI Protection Policy Statement, which addresses, among other things, the policies and procedures the Company has implemented to safeguard its customer's CPNI. The TSNA Protection Policy Statement was delivered to all employees of TSNA, and explains, among other things, what constitutes CPNI, what requirements apply to the use and/or disclosure of CPNI, TSNA CPNI safeguards, and what kinds of record-keeping and reporting obligations apply to CPNI. The Policy is also provided to new employees as part of their orientation materials and included in the Employee Handbook.

TSNA CPNI Instruction Manual

TSNA has implemented a CPNI Instruction Manual. The TSNA Manual explains to its employees how to implement TSNA's CPNI Policies as outlined in the TSNA Protection Policy Statement. The Manual addresses the following topics:

- The process for verifying a customer's identity;
- What information, if any, can be disclosed to the customer upon a customer request;
- When TSNA employees may use CPNI for marketing purposes,
- What to do if a TSNA employee receives a request for CPNI from law enforcement or any other person other than the customer of record; and
- What to do in the event of CPNI security breach.

Use, Disclosure and Access to CPNI

TSNA does not use, disclose or permit access to its customers' CPNI except as any such use,

disclosure or access is permitted by Section 222 of the Telecommunications Act of 1996. TSNA does not use CPNI to market services to customers outside of the category of service to which the customer already subscribes. TSNA also does not share CPNI with its affiliates, or third parties for any marketing purposes. If, in the future, TSNA seeks to use CPNI to market services to customers that are outside of the category of service to which the customer subscribes or to share CPNI with affiliates or third parties, TSNA will provide notice to its customers advising them of their right to approve or disapprove of the proposed uses of CPNI. TSNA will maintain a list of customer preferences.

All marketing campaigns using CPNI must receive prior approval and must be conducted in accordance with the TSNA Policy Statement and CPNI Manual. TSNA will maintain records of all marketing campaigns that use CPNI in accordance with the FCC's rules.

Call Detail Information

TSNA has implemented a policy prohibiting the release of Call Detail Information to any customer during an in-bound call. If a TSNA employee receives a request for Call Detail Information, he/she may provide that information to the caller by sending the information to the address of record or calling the customer back at the telephone number of record. TSNA's policy on Call Detail Information does not allow an employee to disclose any Call Detail Information to the customer other than the Call Detail Information that the customer already has disclosed.

Safeguarding CPNI

TSNA takes the privacy and security of CPNI seriously. In addition to its Call Detail Information Policy, TSNA has established authentication procedures applicable to incoming calls. TSNA has also established detailed procedures for processing certain account changes, and requires the applicable personnel to notify customers immediately of such account changes. TSNA also has implemented network safeguards, including, but not limited to, encrypting certain data. TSNA does not have retail locations.

Employee Training

TSNA has engaged in targeted training of employees and contractors to communicate the proper use and maintenance of CPNI.

Employee Discipline Program

TSNA has a disciplinary process in place to address any noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated TSNA's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

Notice of Security Breaches

Pursuant to TSNA policies, TSNA employees are required to notify their supervisor (who will notify the legal department) immediately if they discover a security breach that has resulted in the unauthorized use, disclosure, or access to CPNI. TSNA notifies the United States Secret Service and the Federal Bureau of Investigation as well as its affected customers of any breaches in accordance with 47 C.F.R. § 64.2011(e). TSNA maintains a record of all security breaches.

T-Systems North America, Inc.
Customer Proprietary Network Information
Instructional Manual

I. PURPOSE

All employees already should have received and reviewed **T-Systems North America, Inc. Customer Proprietary Network Information Protection Policy**, which is located in your Employee Handbook. If you have misplaced your Employee Handbook, please contact **Human Resources**. The purpose of this document is to explain how to implement that policy. This Manual applies only to T-Systems North America, Inc. Deutsche Telekom North America, Inc. has implemented its own CPNI manual. In particular, this document addresses the following topics:

- The process for verifying a customer's identity;
- What information can be disclosed to the customer upon customer request;
- What account modifications may be made by the customer upon customer request;
- When T-Systems North America, Inc. employees may use CPNI for marketing purposes;
- What to do if a T-Systems North America, Inc. employee receives a request for CPNI from law enforcement or any person other than the customer; and
- What to do if a T-Systems North America, Inc. employee learns of or suspects a breach of a customer's CPNI.

These procedures are designed to protect T-Systems North America, Inc. ("T-Systems") and its customers. Telecommunications companies have become victims of pretexters – persons pretending to be a customer in order to obtain that customer's call detail records. These procedures are designed to prevent anyone other than the customer from gaining access to a customer's account. If you have any concern that the person you are speaking with is not who he or she purports to be, please contact David Friedman at (212) 301-6014; do not release any information to the caller or make any changes to the purported customer's account.

Our customers' privacy is extremely important to us. T-Systems North America, Inc. employees are prohibited from using, sharing, or disclosing CPNI except as specified in the CPNI Protection Policy and this Manual. If you have any questions about the CPNI Protection Policy or this Manual, please contact David Friedman at (212) 301-6014.

Failure to comply with these procedures is grounds for disciplinary action, including potential termination.

II. VERIFICATION

T-Systems personnel must verify a caller's identity on all incoming calls. Please record all information about the call in the customer service log.

Verification Procedures for Account Executives and Service Delivery Managers

- Each customer will be assigned an Account Executive and a Service Delivery Manager at T-Systems North America, Inc. The Account Executive and the Service Delivery Manager will be the customer's primary points of contact for all of the customer's requests. For purposes of this manual only, we will refer to the Account Executives and Service Delivery Managers collectively as the "T-Systems Representative."
- Each customer will designate a point(s) of contact responsible for working with the T-Systems Representative. The customer contacts will be identified in the customer's Customer Service Management Fact Sheet. The customer has the option of defining the authority for each designated point of contact (*e.g.*, a point of contact to handle service-related inquiries, a different point of contact to handle sales-related inquiries, etc.).
- T-Systems North America, Inc. will verify a caller's identity on all incoming calls. Upon receipt of an incoming call, the T-Systems Representative will request the caller's name and company name. All Account Executives and Service Delivery Managers are expected to know each of their customers' points of contact personally. If the T-Systems Representative does not recognize the point of contact (for example, by voice), then he or she must ensure that he/she is speaking with the authorized point of contact through additional verification means, including, but not limited to, obtaining the company's billing and/or service address, or requesting information regarding the company's services that the customer only would be privy to if it had a copy of an invoice in its possession. If the customer is unable to verify the requested details, then the T-Systems Representative may not proceed with the call. In these situations, the T-Systems Representative may call the customer at its **telephone number of record** to discuss the account, but may not release any information during the preceding inbound call.¹
- After verifying the caller's identity, the T-Systems Representative should request the purpose of the call. The T-Systems Representative must confirm that the point of contact has the authority to address the subject of the call. If the point of contact does not have the authority (*e.g.*, the particular point of contact is calling to request service to a new location but only has authority to address billing inquiries) to address the subject matter of his/her call, the T-Systems Representative should ask the caller to have the authorized point of contact call T-Systems North America, Inc.

¹ Terms listed in bold are defined in the appendix.

Verification Procedures for Non-Assigned Account Executives, Service Delivery Managers, or Other T-Systems North America, Inc. Personnel

The verification procedures in this section apply to any T-Systems North America, Inc. employee *other than* the customer's assigned Account Executive and Service Delivery Manager. For example, these procedures apply to Account Executives and Service Delivery Managers who are working with a customer whose dedicated Account Executive or Service Delivery Manager is unavailable. These procedures also will apply to any T-Systems North America, Inc. customer service or Systems Competence Center (also referred to herein as the "call center") employee receiving a call from a T-Systems North America, Inc. customer.

- Step 1: Obtain the full name and company name of the caller.
- Step 2: Obtain the customer account number about which the customer is calling. Using the customer account retrieve the caller's account information.
- Step 3: Verify against the T-Systems Customer Service Management Fact Sheet that the caller is an authorized point of contact for the account, and that the caller has the authority to address the subject of his/her call and verify the caller is an authorized point of access
 - If the caller is an authorized point of contact for the account, please proceed to Step 4.
 - If the caller is not an authorized point of contact for the account or does not have the authority to proceed with his/her request, then please inform the caller that (1) he or she is not listed as an authorized point of contact for the account, (2) only the authorized user listed on the account is authorized to receive account information or make changes to the account, and (3) you would be happy to assist the authorized point of contact. ***Please do not release the name of the authorized point of contact. Please do not release any information to the caller.***
 - If the caller informs you that the authorized point of contact has changed, then please inform the caller that he/she must make a change to the authorized point of contact in writing on company letterhead and that you cannot discuss the account with him or her until that change has been made. Please see Part IV "Account Modifications" for additional information.
- Step 4: If the customer has satisfied each of the above questions, then please ask the caller how you can assist him or her. Please refer to the appropriate section below, which explains how to respond to various customer requests.

If you receive a call from a customer and you are neither an Account Executive, a Service Delivery Manager, or a Systems Competence Center employee, please refer the caller to the customer service department for assistance. If you are an employee in the Systems Competence Center and you receive a customer request to address a non-service-related problem, please refer the caller to the customer service department for assistance.

III. DISCLOSING CALL DETAIL INFORMATION UPON CUSTOMER REQUEST

Once T-Systems North America, Inc. has verified a customer's identity using the procedures discussed above, the T-Systems Representative may discuss certain information about the account with the caller. The T-Systems Representative also may make certain changes to the account as outlined in Part IV of this document.

All T-Systems personnel, including T-Systems Representatives, are prohibited from releasing **Call Detail Information** (defined below) to any customer during an in-bound call. If a T-Systems Representative receives a request for **Call Detail Information**, he/she may provide that information to the caller by sending the information to the **address of record** or calling the customer back at the **telephone number of record**. *Please note: as discussed in Part IV, an address of record is not valid until it has been associated with the account for at least 30 days. Therefore, if you receive a request for call detail information within 30 days of the customer becoming a T-Systems customer or within 30 days of a change of address request, you must not release the information to the caller by sending it to the new address of record.*

The prohibition on the release of Call Detail Information during an in-bound call does not prevent a T-Systems Representative from addressing routine service and billing disputes during an in-bound call. As long as the customer's point of contact is able to provide the T-Systems Representative with the call detail information necessary to address the service issue, then the T-Systems Representative may assist the customer with the inquiry. The T-Systems Representative simply cannot disclose any call detail information to the customer other than the call detail information that the customer already has disclosed.

If a customer has not received its bill and requests a duplicate copy of the bill, then you may send a copy of the bill via regular mail to the **address of record**.

If the customer claims to have moved to a new location, then please inform the caller that he must submit a change of address request (see Part IV for the procedures to submit such a request) and that you cannot provide the requested billing information until you have received the change of address form.

IV. ACCOUNT MODIFICATIONS

Once T-Systems North America, Inc. has verified a customer's identity using the procedures outlined above, the T-Systems Representative may make certain changes to the account. If you receive a request to make an account modification discussed herein or to add/delete services to an account and you are neither the customer's Account Executive nor Service Delivery Manager, please transfer the caller to the Customer Service Department for assistance.

Under federal law, T-Systems is required to notify its customers immediately of any creation or change of any address of record (whether electronic or postal). T-Systems representatives must confirm all changes to a customer's address of record in writing immediately following the change by sending a letter to the customer at the *previous* address of record. It is T-Systems policy to notify customers of other changes to their accounts as set forth in this section.

Change of Postal Address of Record

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Verify the address of record.
- Step 3: Inform the customer that a change of billing address of record only can be made in writing. Please inform the customer that if he/she would like to continue to change the address, then he/she should send a written request ***on company letterhead*** to the company's Account Executive or Service Delivery Manager. The letter must be signed by an authorized point of contact and must include the following information:
 - Customer name;
 - Account number;
 - Address of record; and
 - New billing address.
- Step 4: The T-Systems Representative should change the address upon receipt of the appropriate documentation. Please ensure that the change of address is communicated to the billing department.
- Step 5: Once T-Systems North America, Inc. has processed the change of address, we will send a confirmation letter to the **old** billing addresses of record notifying the customer that it has changed its address of record.
- ***NOTE: Under federal law, an address of record must be associated with an account for thirty days before it is valid. Therefore, you must wait thirty days before sending any CPNI (such as call detail records or invoices) to the new address of record.***

Addition of Authorized Representative

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Only the authorized point of contact may add an account representative.
- Step 3: Inform the caller that the addition of an authorized point of contact only can be made in writing. Please inform the customer that if he/she would like to continue with the addition of an authorized account representative, then he/she should mail a written request ***on company letterhead*** to their Account Executive or Service Delivery Manager.
- Step 4: The customer's Account Executive or Service Delivery Manager should add the authorized point of contact upon receipt of the appropriate documentation from the customer. After the Account Executive or Service Delivery Manager has updated the account information, it should send a letter to the authorized point of contact confirming the additional point of contact. ***It is imperative that you not release any information to the new point of contact until after T-Systems North America, Inc. has received the request in writing from the customer.***

Change of Authorized Representative

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Verify the name of the previous authorized account representative.
- Step 3: Inform the caller that a change of the account point of contact only can be made in writing. Please inform the customer that if he/she would like to continue to change the name of the account representative, then he/she should mail or fax a written request ***on company letterhead*** to the company's Account Executive or Service Delivery Manager. The letter must be signed and must include the following information:
 - Customer name;
 - Account number;
 - Current billing address;
 - Name of current account point of contact; and
 - Name of new account point of contact.
- Step 4: Send a letter to the current authorized contact(s) at the company's address of record. It is imperative that you not release any information to the new representative until after T-Systems North America, Inc. has received the request in writing from the customer.

Change of Services on the Account

Any request for change of services on the account will be handled by the Account Executive in conjunction with the legal department and must be made in writing.

Request for Disconnection

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Verify that the company point of contact contacting T-Systems North America, Inc. has the authority to process a disconnect.
- Please inform the customer that the authorized point of contact must fax or mail a written request on company letterhead to the company's Account Executive or Service Delivery Manager.

V. USE OF CPNI FOR MARKETING PURPOSES/SHARING CPNI

All marketing campaigns must receive prior approval from Jason Bennett, the Head of Marketing. Jason Bennett will maintain a record of all marketing campaigns that use CPNI in accordance with the FCC's specifications. If you seek approval to use CPNI for marketing purposes, please provide Jason Bennett with a proposed description of the campaign, the CPNI that you intend to use in the campaign, and what products and services you intend to offer in the campaign.

In accordance with T-Systems North America, Inc.'s CPNI Protection Policy, currently all employees are prohibited from using CPNI to market services to customers outside of the category of service to which the customer already subscribes. If T-Systems North America, Inc. later decides to use CPNI to market products and services to customers outside of the category of service to which the customer subscribes, then we will provide notice to our customers advising them of their right to approve or disapprove of the use of their CPNI for certain marketing purposes. Jason Bennett will maintain and manage a list of all customers who wish to and do not wish to be contacted. The legal department will support Jason Bennett in this capacity.

All employees also are prohibited from sharing CPNI with or releasing CPNI to any affiliate or third party for any purpose except as permitted under this manual.

VI. REQUESTS FOR CPNI FROM LAW ENFORCEMENT PERSONNEL AND PERSONS OTHER THAN THE CUSTOMER

All requests for CPNI from any person other than the customer or the customer's authorized representative, including from law enforcement personnel, will be handled by David Friedman, General Counsel. If you receive a written request for CPNI from any person other than the customer or the customer's authorized representative, please forward the request to David Friedman. If you receive an oral request from any person other than the customer or the customer's authorized representative, please ask that person to call David Friedman at (212) 301-6014.

A request for CPNI includes, but is not limited to, a request for a particular customer or customers' call records. A request for CPNI would include, for example, a request from an attorney claiming to have a valid subpoena for the information. A request from law enforcement personnel may come from a federal or state law enforcement agency, including, but not limited to, the United States Department of Justice, the Federal Bureau of Investigation, the Federal Communications Commission, and the police department. For purposes of this category, law enforcement personnel also includes local state agencies, such as the school board. David Friedman will review all requests for CPNI from persons other than the customer or the customer's authorized representative.

It is T-Systems North America, Inc.'s policy not to release any CPNI to any law enforcement personnel or to any person (other than the customer) claiming a right to the information absent a validly issued written subpoena. Any person or entity requesting CPNI orally will be asked to put the request in writing and to direct that request to David Friedman.

VII. SECURITY BREACHES

T-Systems North America, Inc. will maintain a record of all security breaches discovered. T-Systems North America, Inc. will notify the United States Secret Service and the Federal Bureau of Investigation as well as its affected customers of any breaches in accordance with the FCC's rules. For purposes of this manual, a breach has occurred "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." 47

C.F.R. § 64.2011(e). If you believe that a breach has occurred that has resulted in the unauthorized disclosure of CPNI, please contact David Friedman immediately. All notifications will be handled through Mr. Friedman; if you are aware of a security breach or if you suspect a security breach, please do not contact the customer directly. If the customer suspects that there has been a breach, please refer the call to Mr. Friedman.

Appendix

Account information: information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

Address of record: whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

Call Detail Information: any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Communications-related services: telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

Telephone number of record: the telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."